Notice of Allowability	Application No.	Applicant(s)	
	10/686,316	MONTGOMERY, PETER L.	
	Examiner	Art Unit	
	SHIN-HON CHEN	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *Appeal Brief filed on 7/29/08*.

2. ☒ The allowed claim(s) is/are *2,7,8,10,12,14-19,21 and 22*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *20081027* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

/Shin-Hon Chen/
Examiner, Art Unit 2431

DETAILED ACTION

1. Claims 2, 7, 8, 10, 12, 14-19, 21 and 22 are allowed. Claims 2, 7, 8, 10, 12, 14-19, 21 and 22 are re-numbered as claims 1-13.

EXAMINER'S AMENDMENT

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Beatrice L. Koempel-Thomas on 10/27/08.

The application has been amended as follows:

1. (Cancelled).

2. (Currently Amended) A ~~computer system~~ processing system as recited in claim ~~1~~7, wherein the processor ~~is executing~~ executes a cryptographic function and the Montgomery multiplication is used to compute exponentiations in the cryptographic function.

3. (Cancelled).

4. (Cancelled).

7. (Currently Amended) A processing system comprising:

a processor having a set of registers~~, the processor being configured to support SIMD instructions~~; and

the processor executes a set of SIMD instruction~~, executable by the processor,~~ to perform Montgomery multiplication:

$$\text{montmul}(A, B) = \text{rem}((AB - qN)/R, N), \text{ where } q = \text{rem}(AB\,N', R),$$

where A and B are integers, q is a quotient, N is a modulus, R is an integer that is coprime to modulus N, and N' is an integer such that $NN' \equiv 1 \pmod{R}$, wherein the integer B and the modulus N are implemented as arrays, and at least one SIMD instruction is used to update a first array T_1 with multiples of B for computing AB and to update a second array T_2 with multiples of N for computing qN, wherein a first register holds elements of the B and N arrays;

a second register holds an element of the first array T_1 and an element of the second array T_2; and

a third register is used to hold results of the first array T_1 being updated with a multiple of B and the second array T_2 being updated with multiples of N.

10. (Currently Amended) A processing system as recited in claim ~~9~~7, wherein a single SIMD instruction is used to update the first array T_1 and the second array T_2 simultaneously.

12. (Currently Amended) a computer readable storage medium comprising computer-executable SIMD instructions that, when executed, direct a processor to perform Montgomery multiplication, the instructions comprising:

a first SIMD instruction to load elements of array B and N into a first register;

a second SIMD instruction to load elements of arrays T_1 and T_2 into a second register;

a third SIMD instruction to multiple an element in the array B by a first multiple and an element in the array N by a second multiple;

fourth and fifth SIMD instructions to add results of the third SIMD instruction to the array elements loaded by the second SIMD instruction and to any carries saved from a previous iteration;

sixth and seventh SIMD instructions to separate each output of the fifth SIMD instruction into two reduced size results, one that fits into the arrays T_1 and T_2 and another that represents a carry for a next iteration;

an eighth SIMD instruction to update an element of array T_1 and an element of array T_2 in memory; and

an instruction to store the result of the final iteration.

14. (Currently Amended) A computer readable storage medium as recited in claim 12, wherein the SIMD instructions comprise SSE2 instructions.

19. (Currently Amended) One or more computer readable storage media storing computer executable instructions that, when executed by a computer, perform the method as recited in claim 15.

20. (Cancelled).

21. (Currently Amended) A method as recited in claim ~~20~~15, wherein the computing comprises using the Montgomery multiplication to compute exponentiations in a cryptographic function.

22. (Currently Amended) A method as recited in claim ~~20~~15, wherein the computing comprises using SSE2 instructions.

3. The following is an examiner's statement of reasons for allowance:

As per claim 7, the closest prior art of record (Posch) discloses utilizing SIMD for performing execution of Montgomery multiplication. However, Posch does not explicitly disclose a first register holds elements of the B and N arrays; a second register holds an element of the firs array T1 and an element of the second array T2; and a third register is used to hold results of the first array T1 being updated with a multiple of B and the second array T2 being updated with multiples of N.

As per claim 12, the prior art of record individually or in combination does not disclose a first SIMD instruction to load elements of arrays B and N into a first register; a second SIMD instruction to load elements of arrays T1 and T2 into a second register; a third SIMD instruction to multiply an element in the array B by a first multiple and an element in the array N by a second multiple; fourth and fifth SIMD instructions to add results of the third SIMD instruction to the array elements loaded by the second SIMD instruction and to any carries saved from a previous iteration; sixth and seventh SIMD instructions to separate each output of the fifth SIMD instruction into two reduced size results, one that fits into the arrays T1 and T2 and another that represents a carry for a next iteration; and an eighth SIMD instruction to update an element of array T1 and an element of array T2, in memory.

As per claim 15, the prior art of record individually or in combination does not explicitly disclose iteratively performing, for each digit of integer A from right to left: with array T1 being updated by a product of input B times the digit of integer A, determining what multiple of modulus N allows the updated arrays T1, T2 to end with the same digit; and multiplying the

input B by the digit of integer A and multiplying the modulus N by the determined multiple in light of other features disclosed in independent claim 15.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SHIN-HON CHEN whose telephone number is (571)272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Shin-Hon Chen/
Examiner, Art Unit 2431

Shin-Hon Chen
Examiner
Art Unit 2431